JP20

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of

Takanori MASUI et al. Group Art Unit: 2183

Application No.: 10/660,560

Filed: September 12, 2003 Docket No.: 117046

For: INFORMATION PROCESSOR AND INFORMATION PROCESSING METHOD FOR COOPERATIVE OPERATION OF JOB PROCESSOR

CLAIM FOR PRIORITY

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested for the above-identified patent application and the priority provided in 35 U.S.C. §119 is hereby claimed:

Japanese Patent Application No. 2003-081918 filed March 25, 2003.

In support of this claim, a certified copy of said original foreign application:

☒ is filed herewith.

It is requested that the file of this application be marked to indicate that the requirements of 35 U.S.C. §119 have been fulfilled and that the Patent and Trademark Office kindly acknowledge receipt of this document.

Respectfully submitted,

James A. Oliff
Registration No. 27,075

Thomas J. Pardini
Registration No. 30,411

JAO:TJP/mps

Date: December 10, 2004

OLIFF & BERRIDGE, PLC
P.O. Box 19928
Alexandria, Virginia 22320
Telephone: (703) 836-6400

DEPOSIT ACCOUNT USE AUTHORIZATION
Please grant any extension necessary for entry;
Charge any fee due to our Deposit Account No. 15-0461

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　３月２５日

出願番号
Application Number: 特願２００３－０８１９１８
[ST. 10/C]: [ＪＰ２００３－０８１９１８]

出願人
Applicant(s): 富士ゼロックス株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００３年　９月１０日

特許庁長官
Commissioner,
Japan Patent Office
今井康夫

【書類名】　特許願
【整理番号】　FE03-00269
【提出日】　平成15年 3月25日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 12/00
【発明者】
【住所又は居所】　神奈川県海老名市本郷２２７４番地　富士ゼロックス株式会社海老名事業所内
【氏名】　益井　隆徳
【発明者】
【住所又は居所】　神奈川県海老名市本郷２２７４番地　富士ゼロックス株式会社海老名事業所内
【氏名】　佐竹　雅紀
【発明者】
【住所又は居所】　神奈川県海老名市本郷２２７４番地　富士ゼロックス株式会社海老名事業所内
【氏名】　横濱　竜彦
【特許出願人】
【識別番号】　000005496
【氏名又は名称】　富士ゼロックス株式会社
【代理人】
【識別番号】　100075258
【弁理士】
【氏名又は名称】　吉田　研二
【電話番号】　0422-21-2340

【選任した代理人】

【識別番号】　100096976

【弁理士】

【氏名又は名称】　石田　純

【電話番号】　0422-21-2340

【手数料の表示】

【予納台帳番号】　001753

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報処理装置及び方法

【特許請求の範囲】

【請求項１】　指示データに記述された処理記述に従って処理を実行する複数のジョブ処理装置を連携動作させることによりサービスを実現する情報処理装置であって、

前記指示データに記述された処理記述に対し、各ジョブ処理装置の実行対象となる部分に、実行するジョブ処理装置が復号可能に暗号化する暗号処理部と、

前記暗号処理部により処理記述が暗号化された指示データを、前記処理記述の表わす処理を実行するジョブ処理装置に伝達すべく送信する送信部と

を備えることを特徴とする情報処理装置。

【請求項２】　請求項１に記載の情報処理装置であって、

前記暗号処理部は、暗号化の対象とする処理記述より後に処理を実行すべき処理記述の暗号化データを含めて暗号化することを特徴とする情報処理装置。

【請求項３】　請求項１に記載の情報処理装置であって、

前記暗号処理部は、暗号化の対象となる処理記述を実行するジョブ処理装置の公開鍵を用いて暗号化処理を施すことを特徴とする情報処理装置。

【請求項４】　請求項１記載の情報処理装置において、

前記暗号処理部は、各ジョブ処理装置の実行対象となる複数の部分について、それぞれ暗号化することを特徴とする情報処理装置。

【請求項５】　請求項４記載の情報処理装置において、

前記暗号処理部は、部分毎に異なる鍵で暗号化することを特徴とする情報処理装置。

【請求項６】　複数のジョブ処理装置が所定の順序で連携動作することでサービスを実現するシステムにおいて、そのシステムを構成する情報処理装置であって、

処理の内容が記述された処理記述が暗号化された指示データを受信する受信部と、

前記受信部により受信された指示データに含まれる自装置の実行対象となる処

理記述の部分を復号化する復号処理部と、

前記復号処理部により復号化された処理記述を指示データから削除する削除部と、

前記削除部により処理記述が削除された指示データを、次に処理を実行するジョブ処理装置に向けて送信する送信部と

を備えることを特徴とする情報処理装置。

【請求項７】　指示データに記述された複数の処理記述のそれぞれに従って処理を実行する複数のジョブ処理装置を連携動作させることによりサービスを実現するコンピュータが実行する情報処理方法であって、

前記指示データに記述された処理記述に対し、各ジョブ処理装置の実行対象となる部分に、実行するジョブ処理装置が復号可能に暗号化し、

暗号化された指示データを、前記処理記述の表わす処理を実行するジョブ処理装置に伝達すべく送信する

ことを特徴とする情報処理方法。

【請求項８】　複数のジョブ処理装置が所定の順序で連携動作することでサービスを実現するシステムにおいて、そのシステムを構成するジョブ処理装置の少なくとも１つが実行する情報処理方法であって、

処理の内容が記述された処理記述が暗号化された指示データを受信し、

受信された指示データに含まれる自装置の実行対象となる処理記述の部分を復号化し、

復号化された処理記述を指示データから削除し、

処理記述が削除された指示データを、次に処理を実行するジョブ処理装置に向けて送信する

ことを特徴とする情報処理方法。

【請求項９】　指示データに記述された複数の処理記述のそれぞれに従って処理を実行する複数のジョブ処理装置を連携動作させることによりサービスを実現するコンピュータのプログラムであって、

コンピュータに、

前記指示データに記述された処理記述に対し、各ジョブ処理装置の実行対象と

なる部分に、実行するジョブ処理装置が復号可能に暗号化する手順と、

暗号化された指示データを、前記処理記述の表わす処理を実行するジョブ処理装置に伝達すべく送信する手順と

を実行させるためのプログラム。

【請求項１０】　複数のジョブ処理装置が所定の順序で連携動作することでサービスを実現するシステムにおいて、そのシステムを構成するコンピュータのプログラムであって、

コンピュータに、

処理の内容が記述された処理記述が暗号化された指示データを受信する手順と、

受信された指示データに含まれる自装置の実行対象となる処理記述の部分を復号化する手順と、

復号化された処理記述を指示データから削除する手順と、

処理記述が削除された指示データを、次に処理を実行するジョブ処理装置に向けて送信する手順と

を実行させるためのプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ネットワーク上に存在する様々な処理装置を連携させることで、多様な連携処理を実現するための技術に関し、特に連携処理におけるセキュリティ技術に関する。

【０００２】

【従来の技術】

スキャナ、ファクシミリ装置、プリンタ、複写機、及びそれらの機能を統合した複合機をＬＡＮ（ローカルエリアネットワーク）に接続し、パーソナルコンピュータやメールサーバなどの情報処理装置と連携させ、オフィス作業用の各種サービスを提供するワークフローシステムが提案されている。

【０００３】

また近年、インターネット上に散在する各種ウェブアプリケーションを連携させる技術が提案されている。インターネット上にある多様な提供者が提供するアプリケーションサービスを連結して１つのシステムを構成できると、様々な既存サービスを利用することができるのでシステム開発コストが大幅に低減できると期待されている。また、このような連携的なサービスを実現するための共通の基盤としてＸＭＬ(eXtensible Markup Language)等の言語が注目されている。

【０００４】

また、従来のワークフローシステムとしては、特許文献１や特許文献２、特許文献３に示されるものが知られている。

【０００５】

【特許文献１】

特開平０８－１２３７４４号公報

【特許文献２】

特開２００２－０９９６８６号公報

【特許文献３】

特開２００１－２８２９７０号公報

【０００６】

【発明が解決しようとする課題】

連携サービスのためには、個々の処理装置に対し実行すべき処理を示した指示データを送る必要がある。インターネット上の処理装置を利用してワークフローを構成する場合、処理装置に対する指示データがインターネット上を流れることになる。しかしながら、従来のワークフローシステムは、このようなネットワークを流れる指示データのセキュリティに考慮を払っていない。

【０００７】

また、連携サービスにおいて連携動作する複数の処理装置に対する指示データの提供の仕方として、例えばそれらすべての処理装置の指示データを１つの指示書にまとめて各処理装置に伝達する方式が考えられる。このような方式をとった場合、ある処理装置に対する指示データが他の処理装置にも伝わってしまう。すべての処理装置が同一社内のネットワーク上に存在する場合はこれでもさほど問

題はないが、インターネット上にある外部の処理装置に対して他の処理装置への指示データが漏洩することはセキュリティ上好ましくない。

【０００８】

【課題を解決するための手段】

本発明は、指示データに記述された処理記述に従って処理を実行する複数のジョブ処理装置を連携動作させることによりサービスを実現する情報処理装置であって、前記指示データに記述された処理記述に対し、各ジョブ処理装置の実行対象となる部分に、実行するジョブ処理装置が復号可能に暗号化する暗号処理部と、前記暗号処理部により処理記述が暗号化された指示データを、前記処理記述の表わす処理を実行するジョブ処理装置に伝達すべく送信する送信部と、を備える情報処理装置を提供する。

【０００９】

この情報処理装置は、後述する発明の実施の形態における指示入力装置として実現することもできるし、フロー制御装置として実現することもできる。

【００１０】

また本発明の好適な態様では、前記暗号処理部は、暗号化の対象とする処理記述より後に処理を実行すべき処理記述の暗号化データを含めて暗号化する。

【００１１】

また本発明は、複数のジョブ処理装置が所定の順序で連携動作することでサービスを実現するシステムにおいて、そのシステムを構成する情報処理装置であって、処理の内容が記述された処理記述が暗号化された指示データを受信する受信部と、前記受信部により受信された指示データに含まれる自装置の実行対象となる処理記述の部分を復号化する復号処理部と、前記復号処理部により復号化された処理記述を指示データから削除する削除部と、前記削除部により処理記述が削除された指示データを、次に処理を実行するジョブ処理装置に向けて送信する送信部とを備える。

【００１２】

【発明の実施の形態】

以下、本発明の実施の形態（以下実施形態という）について、図面に基づいて

説明する。

【００１３】

図１は、本発明に係るサービス提供システムのシステム構成パターンの一例を示す図である。このシステムは、指示入力装置１０，フロー制御装置２０，及び複数のアプリケーションサーバ２５を含んでいる。

【００１４】

アプリケーションサーバ２５は、他の装置からの要求に応じて所定の処理サービスを提供するサーバである。例えば、サーバ２５の例としては、例えば、文書データベースサーバや、メールサーバ、画像データに対して色変換や回転などの操作を施す画像処理サーバ等を挙げることができる。サーバ２５は、そのような処理サービスを例えばウェブアプリケーションサービス等の形で提供する。

【００１５】

このシステムは、あるサーバ２５で文書を検索し、この結果検索された文書を別のサーバによって電子メールとして送信する、といった具合に、複数のサーバ２５の処理を連携させた連携サービスを提供することができる。

【００１６】

指示入力装置１０は、このシステムに対するユーザの処理指示を入力するための装置である。ユーザは、指示入力装置１０に対し、上述のような連携サービスの実行指示を入力することができる。指示入力装置１０は、例えばパーソナルコンピュータに、ユーザから本システムへの指示の入力を受け付けるためのユーザインタフェースプログラムを組み込んだものでよい。しかしながら、オフィスにおける文書処理サービスを想定すると、情報処理機能や通信機能に加え、紙文書を読み取って電子データ化する機能をも備えるデジタル複合機を指示入力装置１０として用いることが好適である。デジタル複合機は、スキャナ、プリンタ、複写機、ファクシミリ、ネットワーク通信等の機能を併せ持つ。

【００１７】

フロー制御装置２０は、各サーバ２５に対して処理を依頼することで、それら個々のサーバ２５が提供するサービスを連携した連携サービスを実現する。

【００１８】

好適には、指示入力装置１０、フロー制御装置２０及び各サーバ２５は、公開鍵暗号方式に対応しており、各自の秘密鍵、公開鍵を有している。また、指示入力装置１０、フロー制御装置２０及び各サーバ２５は、他の装置１０，２０やサーバ２５の公開鍵を保持しているか、又は必要に応じてネットワーク上の認証局から取得することができる。

【００１９】

図１のシステムでは、ユーザが指示入力装置１０に対して連携サービスの指示を入力すると、指示入力装置１０がその指示内容を示したデータを送る。このデータ（以下ではフロー指示書５０と呼ぶ）を、フロー制御装置２０に送信する。このフロー指示書５０には、連携サービスに関与するすべてのサーバの処理内容の記述と、それら各処理の実行順序の情報が含まれている。フロー指示書５０を受信したフロー制御装置２０は、その指示書５０に従って各サーバ２５を制御することで、その指示書５０が示す連携サービスを実現する。

【００２０】

このとき、フロー制御装置２０は、受信したフロー指示書５０に基づき各サーバ２５への指示書（指示内容を示したデータ）５２を作成し、これら指示書５２を各サーバ２５に送ることで、それらサーバ２５の連携動作を実現する。すなわち、フロー制御装置２０は、フロー指示書５０の記述に従い、次に動作させるべきサーバ２５に対して指示書５２を送信し、これに対してそのサーバ２５から処理終了の通知（及び場合によっては処理結果のデータ）が返ってくると、その次のサーバ２５に対して指示書５２を送信する。

【００２１】

このように図１のシステムは、サーバ２５群がフロー制御装置２０の制御の下に連携するという、いわばスター（星）型のシステム構成をとっている。

【００２２】

次に、図２を参照して、本発明に係るサービス提供システムのシステム構成パターンの別の一例を説明する。図２において、図１に示したシステムの構成要素と同等の構成要素には同一符号を付して説明を簡略化する。

【００２３】

このシステムは、指示入力装置１０と複数のアプリケーションサーバ２５とから構成されている。

【００２４】

図１のシステムが連携制御のためのフロー制御装置２０を有するのに対し、図２のシステムはそのような中央の制御装置を持たず、各アプリケーションサーバ２５自身が連携動作のための制御動作を実行する。このため、指示入力装置１０は、ユーザが指示した連携サービスのために各サーバ２５が実行すべき処理を示したフロー指示書５０を作成し、これを各サーバ２５に送信して実行させる。

【００２５】

図２の構成は、連携サービスを構成する各処理のための各サーバ２５が、それら各処理の順に並んだ、いわばデイジーチェーン（連鎖）型の構成となる。この構成では、サーバ連鎖の中の最初のサーバ２５－１に対して指示入力装置１０から指示書５０を送信すると、これを契機にサービス処理が開始される。そして、サーバ２５－１の処理が終了すると次のサーバ２５－２の処理が開始され、このサーバ２５－２の処理が終了するとその次のサーバ２５－３の処理が開始されるといった具合に、各段階のサーバ２５の間で処理が連携されていく。この場合、各サーバ２５には、指示入力装置１０から直接、又は前段のサーバ２５から指示書５４が送信される。そして、各サーバ２５はその指示書に従って処理を実行するとともに、その指示書に示された次のサーバ２５に対して処理開始の指示又は指示書５４を送信する。このような仕組みで連携が実現される（詳細は後述）。

【００２６】

以上、各サーバ２５の連携の仕組みとして、フロー制御装置２０により集中制御するフロー制御装置介在型と、各サーバ２５が順に次のサーバ２５に処理を受け渡すフロー制御装置非介在型の２つの仕組みを説明した。

【００２７】

次に、連携サービスのために各サーバ２５に送信される指示書５２，５４についての２つのタイプを説明する。

【００２８】

第１は、連携サービスに関与する各サーバ２５に対し、当該サーバ２５への指

示（該サーバ２５の処理内容の記述）のみならず、他のサーバ２５への指示をも含んだ指示書５２又は５４を送信する方式である。この方式の１つの例として、連携サービスに関与するすべてのサーバ２５への指示を含んだ指示書を各サーバ２５に送信する方式がある。このように、他のサーバ２５への指示も含む形態の指示書を「包括指示書」と呼ぶこととする。

【００２９】

第２は、連携サービスに関与する各サーバ２５に対し、当該サーバ２５への指示のみを含み、他のサーバ２５への指示を含まない指示書５２又は５４を送信する方式である。このように、他のサーバ２５への指示を含まないタイプの指示書を「個別指示書」と呼ぶこととする。

【００３０】

これら指示書５２又は５４の２つのタイプと、前述のシステム構成の２つのタイプを組み合わせれば、各サーバ２５への指示書の送信形態としていくつかの送信形態が得られる。そのうちの代表的なものとして次の４つの指示送信形態を挙げることができる。

【００３１】

第１は、フロー制御装置介在型のシステムに包括指示書を適用したものであり、フロー制御装置２０から各サーバ２５に対して包括指示書６０を送信する方式である。この形態の一例を図３に示す。

【００３２】

図３の例では、サーバ２５－１に対する指示内容を示した個別指示書６２－１と、サーバ２５－２に対する指示内容を示した個別指示書６２－２と、サーバ２５－３への指示内容を示した個別指示書６２－３とを含んだ包括指示書６０を、フロー制御装置２０からそれら各サーバ２５－１，２５－２，２５－３に送信する。この包括指示書６０では、各個別指示書６２が処理の実行順序に従って先頭から順に並べられている。この包括指示書６０は、指示入力装置１０からフロー制御装置２０に送られるフロー指示書５０の記述内容に基づき作成される。例えば、フロー指示書５０は包括指示書６０と同じ内容を記述したものでよい。

【００３３】

この場合、フロー制御装置２０は、まず連携サービスの最初のサーバ２５－１に対して包括指示書６０を送信する。サーバ２５－１はその包括指示書６０のうち自分宛の個別指示書６２－１を解釈して処理を実行し、その処理結果をフロー制御装置２０に返す。これを受けたフロー制御装置２０は、次のサーバ２５－１に対して包括指示書６０を送信する。このような処理を繰り返すことで連携サービスを実現できる。

【００３４】

この変形として、フロー制御装置２０から各サーバ２５に送信する包括指示書６０から、それまでに完了している処理についての記述を取り除く方式も好適である。この構成によれば、少なくとも処理が終わったサーバ２５の処理内容は、後続のサーバ２５に対して秘密にすることができる。

【００３５】

また、図３の指示送信形態の別の変形として、次のような方式も可能である。この方式では、まず連携サービスに関与するすべてのサーバ２５への個別指示書６２を含んだ包括指示書６０をフロー制御装置２０からそれら各サーバ２５に送信する。そして、各サーバ２５は、自分の前のサーバ２５から処理開始指示が来るまでは処理を開始せず、その開始指示を受け取ると包括指示書６０内の自分宛の個別指示書６２に従って処理を実行し、自分の処理が終わるとその旨をフロー制御装置２０に通知する。フロー制御装置２０は、その通知を受けると、次のサーバに処理開始指示を出す。

【００３６】

第２の指示送信形態は、フロー制御装置介在型システムに個別指示書を適用したものであり、フロー制御装置２０から各サーバ２５に対し、それぞれ当該サーバ２５に対応する個別指示書６２を送信する。この一例を図４に示す。

【００３７】

図４の例では、フロー制御装置２０は、指示入力装置１０から受信したフロー指示書に基づき、サーバ２５－１に対する指示内容を示した個別指示書６２－１と、サーバ２５－２に対する指示内容を示した個別指示書６２－２と、サーバ２５－３への指示内容を示した個別指示書６２－３とをそれぞれ作成し、それら各

個別指示書６２をそれぞれ対応するサーバ２５に送信する。

【００３８】

第３の指示送信形態は、フロー制御装置非介在型システムに包括指示書を適用したものである。この形態の一例を図５に示す。

【００３９】

図５の形態では、図３の形態と同様の包括指示書６０を、サーバ２５－１からサーバ２５－２へ、サーバ２５－２からサーバ２５－３へと受け渡す。すなわち、図５の例では、まず指示入力装置１０からサーバ２５－１に対し、包括指示書６０と同内容のフロー指示書を送信する。サーバ２５－１は、包括指示書６０の中の自分宛の個別指示書６２－１に示される処理を実行し、その処理が完了すると、同じ包括指示書６０（及び必要に応じてその処理の結果）を次のサーバ２５－２に送信する。サーバ２５－２は、包括指示書６０を受け取ると、自分宛の個別指示書６２－２に示される処理を実行し、その処理が完了すると、同じ包括指示書６０（及び必要に応じてその処理の結果）を次のサーバ２５－３に送信する。このようにして、各サーバ２５による処理の連携が実現される。

【００４０】

図５の指示送信形態の変形として、各サーバ２５が処理を終えると、自分が実行した処理についての記述（すなわち自分宛の個別指示書６２）を包括指示書６０から取り除き、残りの個別指示書６２からなる包括指示書を作成して次のサーバ２５に送信する構成も好適である。この構成によれば、少なくとも処理が終わったサーバ２５の処理内容は、後続のサーバ２５に対して秘密にすることができる。

【００４１】

また、図５の送信指示形態の別の変形として、次のような方式も可能である。この方式では、まず連携サービスに関与するすべてのサーバ２５への個別指示書６２を含んだ包括指示書６０を指示入力装置１０からそれら各サーバ２５に送信する。そして、各サーバ２５は、自分の前のサーバ２５から処理開始指示が来るまでは処理を開始せず、その開始指示を受け取ると包括指示書６０内の自分宛の個別指示書６２に従って処理を実行し、自分の処理が終わると次のサーバに処理

開始指示を出す。包括指示書６０では、各サーバ２５の個別指示書６２が処理の順に並んでいるので、各サーバ２５は前後の個別指示書６２の記述から自分の前段のサーバ２５や後段のサーバ２５を識別することができ、上記のような処理の流れを実現できる。

【００４２】

第４の指示送信形態は、フロー制御装置非介在型システムに個別指示書を適用した方式である。この方式の一例を図６に示す。

【００４３】

図６の例では、指示入力装置１０から、連携サービスに関与する各サーバ２５－１，２５－２，２５－３に対し、それぞれ当該サーバ２５に対応する個別指示書６２－１，６２－２，６２－３を送信する。そして、各サーバ２５宛の個別指示書６２には、当該サーバ２５の前後の各サーバ２５（又は指示入力装置１０）を示す情報が含まれている。そして、各サーバ２５は、前段のサーバ２５から処理開始指示を受けて初めてその個別指示書６２の処理を開始し、処理が終了すると後段のサーバ２５に対して処理開始指示を送る。このような仕組みにより、サーバ２５間の連携を実現できる。

【００４４】

以上に説明した指示送信形態のうち、各サーバ２５に個別指示書６２を送信する第２及び第４の形態では、インターネット等のネットワーク上で個別指示書６２の内容を盗聴されるリスクがある。

【００４５】

また、各サーバ２５に包括指示書６０を送る第１及び第３の形態では、ネットワーク上での盗聴のリスクに加え、各サーバ２５への指示内容が他のサーバ２５に漏洩するリスクがある。例えば、ある企業が連携サービスのために、自社のサーバ２５以外に他社が提供するインターネット５０上のサーバ２５を用いる場合、自社サーバ２５への指示内容が他社サーバ２５に知られたくないことが少なくない。

【００４６】

以下、このような各サーバ２５に送る指示書についてのセキュリティ上のリス

クを軽減するための仕組みについて説明する。

【００４７】

この仕組みの基本的な考え方は、サーバ２５に対する個別指示書６２に対し、連携サービスに関与するサーバ２５群の中でそのサーバ２５のみが復号可能な暗号化処理を施すというものである。

【００４８】

各サーバ２５に対して対応する個別指示書６２のみを送信する上記第２及び第４の指示送信形態では、このような暗号化により、ネットワーク上での指示内容の漏洩リスクを軽減できる。

【００４９】

また、各サーバ２５に対して包括指示書６０を送信する上記第１及び第３の指示送信形態では、包括指示書６０に含まれるべき各個別指示書６２に対し、それぞれ対応するサーバ２５にのみ復号可能な暗号化処理を施し、それら暗号化された個別指示書を処理実行順序に従って並べた包括指示書６０を作成する。これにより、各サーバ２５に対する個別指示書６２の内容がネットワーク上で盗聴されるリスクを軽減できると共に、他のサーバ２５に漏洩するリスクも軽減できる。

【００５０】

いずれの場合も、個別指示書６２の暗号化処理としては、共通鍵暗号方式を利用した暗号化処理を用いることもできるし、公開鍵暗号方式を利用した暗号化処理を用いることもできる。共通鍵暗号方式を用いる場合は、各サーバ宛の個別指示書６２を作成するフロー制御装置２０又は指示入力装置１０と、当該指示書６２の送り先のサーバ２５とが、暗号・復号化のための共通鍵を有していればよい。一方、公開鍵暗号方式を用いる場合は、各サーバ２５宛の個別指示書６２を作成するフロー制御装置２０又は指示入力装置１０が、それら各サーバ２５の公開鍵を有しているか、それら公開鍵をネットワーク上の鍵管理サーバや認証局から取得する機能を有していればよい。また、個別指示書６２を暗号化するセッション鍵（共通鍵）を乱数から生成して、そのセッション鍵で個別指示書６２を暗号化すると共に、その暗号化されたセッション鍵を各サーバ２５の公開鍵で暗号化して、暗号化された個別指示書６２と一緒に送付してもよい。

【００５１】

なお、フロー制御装置２０を用いる上記第１及び第２の指示送信形態では、処理の開始に当たり、指示入力装置１０からフロー制御装置２０に対してフロー指示書５０を送る必要がある。この場合、指示入力装置１０が、フロー制御装置２０のみが復号可能な暗号化処理（例えばフロー制御装置２０の公開鍵を用いた暗号化）を用いてそのフロー指示書５０を暗号化し、この結果得られる暗号化された指示書をフロー制御装置２０に送信する。フロー制御装置２０は、受け取った指示書を復号し、この復号化結果に基づき各サーバ２５宛の個別指示書６２（第２又は第４の形態）又は包括指示書６０（第１又は第３の形態）を作成する。

【００５２】

次に、連携サービスの具体例を用いて、本実施形態における指示書の暗号化処理について説明する。

【００５３】

ここでは、具体例として、図７に示すように、ページばらし（文書ファイルをページ単位のファイルに分割し、要求されたページのファイルを返す処理）のサービスを提供するサーバ２５ａと、電子メール送信サービスを提供するサーバ２５ｂを含むシステムを想定する。サーバ２５ａは”pagedivider.foo.jp”というホスト名を有し、サーバ２５ｂは”mailsender.foo.jp”というホスト名を有するとする。そして、このシステムで、指示入力装置１０で読み取った複数のページを有する紙原稿のうちの第１ページのデータを、所定の宛先に電子メールで送信するというサービス（以下、便宜上「サービスＡ」と呼ぶ）を実現するとする。サービスＡでは、指示入力装置１０にて紙原稿の読み取りが行われ、サーバ２５ａにて読み取り結果の文書ファイルから第１ページが抽出され、サーバ２５ｂにてその第１ページのファイルを含んだ電子メールが作成され、所定宛先に送られることになる。また、この例では、指示送信形態として、図５に例示した第３の形態を用いるものとする。

【００５４】

この場合、指示入力装置１０は、そのサービスＡの内容を示す包括指示書６００を作成する。図８に、この包括指示書６００の例を示す。

【００５５】

この例の包括指示書６００は、ＸＭＬ(eXtended Markup Language)で記述されている。この包括指示書６００は、この指示書６００で使用しているＸＭＬのバージョンや文字コードを示す文書要素６０５と、この指示書６００が表す連携サービスを示す文書要素６１０とを含んでいる。連携サービスを示す要素６１０のタグには、この連携サービスの名称（name="report delivery"）が示されている。そして、この要素６１０には、それら連携サービスを担う各サーバ２５ａ，２５ｂに対する個別指示書６２０ａ，６２０ｂとが記述されている。

【００５６】

個別指示書６２０ａの記述６２２ａには、連携サービス中での当該処理の順番（order="1"）、及び当該処理を実行するサーバ２５ａのホスト名（url="pagedivider.foo.jp"）が示されている。また、記述６２４ａの１行目には、そのサーバ２５ａが提供する各種の処理のうち、今回利用する処理の名称（jobname="ExtractFrontPage"）が示される。例えば、サーバ２５ａは、文書ファイルから先頭ページを取り出してその先頭ページのファイルを作成する処理の他に、文書ファイルをページ単位にばらして各ページごとのファイルを作成する処理などの様々な処理ができる。記述６２４ａの１行目は、それら様々な処理のうち、文書ファイルの先頭ページのファイルを作成する処理を示すものである。また記述６２４ａの２行目及び３行目にはその処理のパラメータが示されている。２行目のパラメータは、その処理に対する入力ファイルのファイル名（"ExtractFrontPage"）を示し、３行目のパラメータはその処理の出力ファイルのファイル名（"ExtractedPage"）である。指示入力装置１０が、読み取った原稿を示す文書ファイルに対し、"ExtractFrontPage"というファイル名を付し、この指示書６００に添付して送信すれば、サーバ２５ａでそのファイルが処理対象であると認識できる。

【００５７】

また、個別指示書６２０ａは、この指示書が示す処理の後に処理を行うサーバ２５ｂを示す記述６２６ａを含んでいる。この記述６２６ａには、次のサーバ２５ｂのホスト名（url="pagedivider.foo.jp"）が示されている。

【００５８】

サーバ２５ｂに対する個別指示書６２０ｂは、上記個別指示書６２０ａと同様、処理の順序及びサーバ２５ｂのホスト名を示す記述６２２ｂと、そのサーバ２５ｂが行うべき処理の名称及びその処理のパラメータを示す記述６２４ｂを含んでいる。サーバ２５ｂが行う処理は、電子メールの送信処理なので、パラメータとしては電子メールの宛先アドレス（記述６２４ｂの２行目）と、その電子メールに添付されるファイルの名称（記述６２４ｂの３行目）とを含んでいる。なお、添付されるファイルの名称は、サーバ２５ａの処理の出力ファイル名と同じものとなっている。

【００５９】

なお、サーバ２５ｂは、この包括指示書６００が示す連携サービスの中の最後の処理なので、次のサーバを示す記述は含まれていない。

【００６０】

図８に示した包括指示書６００では、各個別指示書６２０ａ，６２０ｂ内の処理内容を示す記述６２４ａ，６２４ｂが平文で記述されているので、このままネットワーク上に送信すると、盗聴のリスクがあるとともに、２番目のサーバ２５ｂの処理内容が最初のサーバ２５ａに知られてしまうことになる。例えば、処理内容の記述の中に、ユーザのクレジットカード番号などがパラメータとして含まれる場合などには、その情報が関係するサーバ以外に漏れることは望ましくない。また、その処理内容全体を関係するサーバ以外に秘匿したい場合もある。

【００６１】

そこで、図７の例では、指示入力装置１０が、その包括指示書６００の各個別指示書６２０ａ，６２０ｂのうちの処理内容を示す記述６２４ａ，６２４ｂを、それぞれ対応するサーバ２５ａ，２５ｂの公開鍵を用いて暗号化する。このような暗号化処理を経た包括指示書の例を図９に示す。図９において、図８と同内容の記述には、図８と同じ符号を付して説明を省略する。

【００６２】

図９に示す包括指示書７００は、Ｗ３Ｃの規格である“ＸＭＬ　Ｅｎｃｒｙｐｔｉｏｎ”に従ったものである。この包括指示書７００において、サーバ２５ａに対する個別指示書７２０ａは、処理の順序及びサーバ２５ｂのホスト名を示す

記述６２２ａと、次に処理を行うサーバ２５ｂを示す記述６２６ａと、暗号化部分７２４ａとを含んでいる。この暗号化部分７２４ａは、平文の個別指示書６２０ａの処理内容の記述６２４ａを、サーバ２５ａの公開鍵を用いて暗号化したデータを含む。記述７２５ａのタグ"<CipherValue>"と"</CipherValue>"とに挟まれたASCIIコードの文字列が、その暗号化データの値を示している。暗号化部分７２４ａの最初のタグには、その暗号化データを生成するのに使用した暗号化方式を示す情報（"Type='http://www.w3.org/2001/04/xmlenc#Element' xmlns='http://www.w3.org/2001/04/xmlenc#'"）が記述されている。なお、説明を簡単にするために図９では省略しているが、この暗号化データを生成するのに用いた公開鍵を示す鍵情報の要素（"<KeyInfo>"）がその暗号化部分７２４ａ内に記述されている。

【００６３】

同様に、サーバ２５ｂに対する個別指示書７２０ｂには、処理の順序及びサーバ２５ｂのホスト名を示す記述６２２ｂと、処理内容６２４ｂをサーバ２５ｂの公開鍵で暗号化したデータの記述７２５ｂを含んだ暗号化部分７２４bとを有する。

【００６４】

図９に示した包括指示書７００を用いれば、ネットワーク上で仮にその包括指示書７００が盗聴されても、各サーバ２５ａ、２５ｂの処理内容はその暗号が解読されない限り知られない。また、サーバ２５ａやサーバ２６ｂがこの包括指示書７００を受け取った場合、自分宛の個別指示書の暗号化部分７２４ａ、７２４ｂは自分の秘密鍵で復号できるが、他のサーバに対する個別指示書の暗号化部分は復号できない。

【００６５】

図７のシステムでは、指示入力装置１０が、上述の包括指示書７００を作成し、付属のスキャナで読み取った原稿の文書ファイルをその指示書７００と共にサーバ２５ａに送信する。これらのデータを受け取ったサーバ２５ａは、指示書７００中の処理順序及びホスト名の記述６２２ａ及び６２２ｂの平文記述を調べることで、自分宛の個別指示書６２０ａを識別する。次にその個別指示書６２０ａ

の中の暗号化部分７２４ａを自分の秘密鍵で復号する。この復号結果は、図８に示した処理内容の記述６２４ａとなる。そして、暗号化部分７２４ａを復号結果の記述６２４ａに置き換えることで、平文の個別指示書６２０ａを復元し、この指示書６２０ａを先頭から順に解釈していき、その解釈に応じた処理を実行する。この例では、サーバ２５ａは、入力された文書ファイルから先頭ページを取り出す処理を実行し、その先頭ページのファイルに所定のファイル名"ExtractedPage"をつける。このようにして、要求されたサービス処理を完了すると、サーバ２５ａは、作成した先頭ページのファイルと包括指示書７００とを、記述６２６ａに従って次のサーバ２５ｂに送信する。

【００６６】

サーバ２５ｂは、サーバ２５ａと同様に、受け取った包括指示書７００から自分宛の個別指示書７２０ｂを識別し、その中の暗号化部分７２４ｂを自分の秘密鍵で復号することで平文の個別指示書６２０ｂを復元し、その平文指示書６２０ｂに示された処理を実行する。この場合サーバ２５ｂは、先頭ページのファイル"ExtractedPage"を添付した電子メールを作成し、平文指示書６２０ｂに記述された宛先（"personl@foo.co.jp"）に対して送信する。

【００６７】

以上では、説明を分かりやすくするために非常に単純な例を挙げたが、もっと複雑な処理にも本実施形態の仕組みは適用可能である。例えば、この例の拡張として、例えばユーザが読み取った文書の先頭ページをユーザの属するグループのリーダに、全ページをそのグループの同僚複数人に送信するといった定型処理も同様に実現可能である。この場合は、サーバ２５ａに対する個別指示書６２０ａには、文書ファイルから第１ページを抽出すると共に、第１ページのファイルとその文書ファイルとをサーバ２５ｂに送るという処理内容が記述され、サーバ２５ｂに対する個別指示書６２０ｂには、受け取った第１ページのファイルをグループリーダの所定のメールアドレスに送信し、全ページのファイルを各同僚の所定のメールアドレスに送信するという処理内容が記述される。暗号化については、上記の例と同様でよい。

【００６８】

このような仕組みによれば、各個別指示書６２０ａ，６２０ｂの処理内容が第三者に盗聴されたり、その処理を実行するサーバ以外のサーバに漏れたりする可能性を大幅に低減できる。

【００６９】

なお、以上のシステムにおいて、指示入力装置１０がサーバ２５ａの処理の対象である文書データをそのサーバ２５ａの公開鍵で暗号化してから送信したり、サーバ２５ａがサーバ２５ｂの処理の対象である先頭ページのデータをそのサーバ２５ｂの公開鍵で暗号化したりすれば、それら処理対象のデータをネットワーク上の第三者から保護することが可能である。

【００７０】

以上に説明した図９の例では、各個別指示書の処理内容の記述６２４ａを暗号化したが、次のサーバの示す記述６２６ａを併せて暗号化しても問題ない。個別指示書は、その個別指示書がどのサーバ宛のものなのかが特定できる情報のみ平文で記述しておけば、他の情報についてはすべて暗号化しても構わない。

【００７１】

また、サーバ２５ａは、次のサーバ２５ｂに包括指示書７００を送る代わりに、その包括指示書７００から自分宛の個別指示書７２０ｂを除いた指示書を作成し、これをサーバ２５ｂに送る構成としても良い。

【００７２】

図７～図９に示した例は、指示送信形態として、図５に例示した第３の形態を用いた場合の例であったが、図３に示した第１の形態を用いる場合もこれと同様、図９に示すような暗号化された包括指示書７００を各サーバ２５に送るようにすればよい。ただし、このケースでは、各個別指示書の暗号化はフロー制御装置２０にて行うこともできる。この場合、指示入力装置１０は、フロー制御装置２０に対し、包括指示書６００の連携サービスを示す文書要素６１０全体をそのフロー制御装置２０の公開鍵で暗号化したものを送信することで、包括指示書６００全体の秘密を保持することができる。フロー制御装置２０はそれを自分の秘密鍵で復号したあと、個々の個別指示書６２０ａ、６２０ｂを対応するサーバ２５ａ，２５ｂの公開鍵で暗号化し、包括指示書７００を作成する。この包括指示書

７００を用いた各サーバ２５の制御は、上述の通りでよい。

【００７３】

また図４に示した第２の指示書送信形態を用いる場合は、各サーバ２５には個別指示書のみを送ればよいので、フロー制御装置２０にて、その個別指示書の中の処理内容等の記述を宛先のサーバ２５の公開鍵で暗号化すればよい。この暗号化により生成される個別指示書の記述は、例えば、図９に示した包括指示書７００を、個別指示書７２０ａを１つしか含まないようにしたものでよい。

【００７４】

図６に示した第４の指示書送信形態を用いる場合も各サーバ２５には個別指示書のみを送ればよいので、指示入力装置１０にて、第２の形態と同様、その個別指示書の中の処理内容等の記述を宛先のサーバ２５の公開鍵で暗号化すればよい。

【００７５】

以上、本実施形態における、各指示送信形態に対応する指示書データの秘密保護の方式について説明した。

【００７６】

次に、包括指示書６０の変形例について説明する。この変形例の包括指示書は、特に第３の指示送信形態において有益なものである。

【００７７】

図１０は、この変形例における包括指示書８０のデータ構造を説明するための図である。この指示書８０が適用されるシステム構成は、図５を参照されたい。

【００７８】

この包括指示書８０は、連携サービスの各処理を担う各サーバ２５－１，２５－２，２５－３に対する各個別指示書６２－１，６２－２，６２－３を、それら各処理の順序に従った入れ子構造となるように暗号化する。

【００７９】

より詳しくは、まず連携サービスのフローの最後のサーバ２５－３宛の個別指示書６２－３を該サーバ２５－３の公開鍵で暗号化し、暗号化データ８２－３を作成する。この暗号化では、個別指示書６２－３のうち、この指示書の処理を実

行するサーバを示す記述（例えば図８の記述６２２ａ）を除く部分を暗号化する。もちろん、暗号化する箇所をその部分よりも更に絞り込んでもよい。

【００８０】

次に、最後のサーバ２５－３の１つ前のサーバ２５－２宛の個別指示書６２－２と、その暗号化データ８２－３とを併せたものを、サーバ２５－２の公開鍵で暗号化することで、暗号化データ８２－２を作成する。

【００８１】

そして、その１つ前のサーバ２５－１宛の個別指示書６２－１とその暗号化データ８２－２とを併せたものを、サーバ２５－１の公開鍵で暗号化することで、暗号化データ８２－１を作成する。

【００８２】

このような処理を、連携サービスのフローにおける先頭のサーバの個別指示書を暗号化するまで再帰的に繰り返す。すなわち、この暗号化処理では、暗号化の対象とする処理記述（すなわち個別指示書）に、その記述より後に処理を実行すべき処理記述の暗号化データを含めて暗号化する。そして、この暗号化処理を、実行順序が最後の処理記述から順に再帰的に適用する。

【００８３】

図１０の例では、サーバ２５－１が先頭のサーバなので、この暗号化の最終結果は暗号化データ８２－１となる。この最終の暗号化データ８２－１に対し、連携サービスの指示書である旨を示す記述（図８の記述６０５や文書要素６１０の開始タグ及び終了タグ）を付加することで、包括指示書８０が完成する。

【００８４】

この入れ子構造の包括指示書の具体例を図１１に示す。この例は、図８に示す平文の包括指示書６００に対応するものである。この指示書が適用されるシステム構成としては、図７の構成を参照されたい。

【００８５】

図１１に示す包括指示書８００は、ＸＭＬのバージョン等の記述６０５と連携サービスの名称の記述６１５の後に、入れ子構造で暗号化された暗号化データ８２０を含む文書要素８１０を含んでいる。この文書要素８１０の先頭には、連携

サービスの先頭のサーバ２５ａのホスト名を含んだタグ８１５が示されている。暗号化データ８２０は、使用した暗号方式を示す記述と、入れ子構造の暗号化の最終的な暗号化結果の値の記述８２５を含んでいる。

【００８６】

指示入力装置１０は、このような包括指示書８００を作成し、連携サービスの先頭のサーバ２５ａに送信する。これを受信したサーバ２５ａは、平文で記述された"<wrapinstruction>"タグ８１５内のホスト名から、その指示書８００が自分宛であることを認識し、その中の記述８２５に示される暗号化結果の値を自分の秘密鍵を用いて復号する。これにより、復号結果８３０が得られる。

【００８７】

復号結果８３０は、そのサーバ２５ａ宛の平文の個別指示書６２０ａと、後続のサーバ２５群宛の入れ子構造の暗号化データ８５０を含んだ文書要素８４０が含まれる。

【００８８】

サーバ２５ａは、その平文の個別指示書６２０ａに従って処理を実行する。そして、処理が完了すると、記述６２６ａに示される次のサーバ２５ｂに対する指示書を作成し、その指示書とその処理の結果とをサーバ２５ｂに送信する。このとき、次のサーバ２５ｂへの指示書は、復号結果８３０から処理済みの自分宛の個別指示書６２０ａを削除することで作成できる。すなわち、その指示書には、指示書であることを示す記述６０５及び６１５と、暗号化データ８５０を含む文書要素８４０が含まれることになる。

【００８９】

この指示書を受け取ったサーバ２５ｂは、その文書要素８４０中に含まれるホスト名の記述６２２ｂからその指示書が自分宛であることを認識し、記述８５５に含まれる暗号化結果の値を自分の秘密鍵で復号する。これにより、図７の指示書における、処理内容の記述６２４ｂ（図８参照）に対応する平文記述を得ることができる。サーバ２５ｂは、その記述６２４ｂに従って処理を実行する。

【００９０】

なお、図１１の例では、サーバ２５ｂが連携サービスの最後のサーバであった

ため、文書要素８４０は"<service>"タグで示される文書要素として表された。このかわりに、サーバ２５ａの次のサーバ２５ｂが連携サービスの最後でなければ、文書要素８４０は、最初の包括指示書８００の文書８１０と同様、"<wrapinstruction>"タグによって示されることとなる。なお、連携サービスの最後のサーバ宛の個別指示書も、他のサーバ宛の各段階の暗号化結果と同様、指示書全体を暗号化し、その暗号化結果"<wrapinstruction>"タグで囲むようにしてももちろんよい。

【００９１】

このように、指示入力装置１０で入れ子構造の包括指示書８００を作成する構成とすれば、あるサーバ宛の個別指示書は連携サービスのフローの中でそのサーバより前のすべてのサーバにより順に復号処理を受けない限り復号できない。したがって、連携サービスの先頭のサーバ以外のあるサーバＸが、自分の前段のサーバ以外から予め包括指示書を取得したとしても、そのサーバＸは復号ができないので処理を開始することができない。

【００９２】

このような仕組みを利用すれば、あるサーバＸが、連携サービスのフローに従った処理を経ずに、勝手に処理を始めてしまうことを防止することができる。例えば、サーバＸが課金を伴う処理を行う場合、正しい処理フローを経ずに、前もって処理を始めて課金を開始すると、連携サービスを要求したユーザにとって好ましくないが、この入れ子構造の包括指示書８００を用いることで、そのような状況が起こるのを抑止できる。

【００９３】

以上、本実施形態のシステムの構成及び動作について説明した。以上の実施形態では、連携サービスのための個々の処理についての指示を、その処理を実行するサーバ２５のみが復号可能な暗号処理で暗号化した。このときの暗号処理の単位となる「サーバ」は、あるサービス処理を記述したアプリケーションプログラムをコンピュータで実行させることにより実現される仮想機械であってもよいし、そのようなアプリケーションプログラムを１乃至複数備えたハードウエア装置であってもよい。すなわち、前者の場合アプリケーションごとに異なる暗号処理

を用い、後者の場合はハードウエア装置ごとに異なる暗号処理を用いることになる。アプリケーションごとの異なる暗号処理の例としては、アプリケーションごとにそれぞれ個別に秘密鍵・公開鍵ペアを割り当てて、公開鍵暗号方式を用いる仕組みを挙げることができる。ハードウエア装置ごとに異なる暗号化処理も同様である。ハードウエア装置単位の暗号処理を採用する場合、ハードウエア装置に対する個別指示書としては、連携サービス中でハードウエア装置内の各アプリケーションが連続して実行する処理の内容を順に記述したものとなる。指示入力装置１０又はフロー制御装置２０は、その個別指示書をそのハードウエア装置に対応する暗号処理にて暗号化する。

【００９４】

次にこのシステムを構成する指示入力装置１０，フロー制御装置２０及び各サーバ２５の内部構成の一例を、図１２を参照して説明する。

【００９５】

まず、指示入力装置１０について説明する。指示入力装置１０のＵＩ（ユーザ・インタフェース）１０２は、指示入力装置１０の状態や操作メニュー等を表示し、これに対するユーザの選択やパラメータ入力を受け取るユーザ・インタフェース機構であり、例えば液晶タッチパネルやテンキーボタン、各種の指示ボタンを備える。処理モジュール１０４は、当該指示入力装置１０自体がユーザに提供するサービス処理を実行する処理モジュールである。指示入力装置１０が複合機である場合、処理モジュール１０４には、スキャン機能、プリント機能、コピー機能、ファクシミリ送受信機能等を実現する機能モジュールが含まれる。この場合、これら処理モジュール１０４は、スキャンエンジンやプリントエンジン、ファクシミリ装置等のハードウエアと、それら各ハードウエアを制御するソフトウエアの組合せにより構成される。通信制御部１０６は、この指示入力装置１０とＬＡＮ等のネットワーク３５上の他の装置との通信のための各種制御処理を行う機能モジュールである。

【００９６】

暗号・復号処理部１０８は、指示入力装置１０からネットワーク３５に送信するデータに対して暗号化を行ったり、送信されてきた暗号化されたデータを復号

したりする機能モジュールである。ここでは、暗号・復号処理部１０８は、暗号方式として公開鍵暗号方式をサポートしているものとする。ただし、これは一例であり、暗号・復号処理部１０８は、共通鍵方式など他の暗号方式を基礎とするものであってもよい。

【００９７】

暗号・復号処理部１０８で用いる暗号化処理の一例としては、乱数等で発生したセッション鍵（共通鍵）を用いて対象となる文書データを暗号化し、このセッション鍵を送信先の公開鍵で暗号化し、これら両暗号化データを送信先へに送信するという処理を挙げることができる。受信側では、受け取ったデータを自らの秘密鍵で復号することでセッション鍵を得、暗号化された文書データをそのセッション鍵により復号する。本明細書中で「公開鍵で暗号化する」といった場合、文字通り公開鍵を用いて対象データを暗号化する場合のみならず、このようなセッション鍵を利用する暗号化処理の場合もあるものとする。

【００９８】

また、暗号・復号処理部１０８は、送信するデータに対して電子署名を施したり、受信したデータに付された電子署名を検証したりする機能を備える。電子署名は、例えば署名対象の文書データからＭＤ５(RFC1321)やＳＨＡ－１(RFC3174)等の所定ダイジェスト方式に従って求めたメッセージダイジェストを、署名者の秘密鍵で暗号化することにより得られる。この電子署名の検証は、該署名データを署名者の公開鍵で復号し、その復号化結果が、署名対象の文書データから所定ダイジェスト方式に従って求めたメッセージダイジェストと一致するか否かを判定することにより行われる。一致すれば、該文書データが署名者からの真正なデータであることが証明されると共に、該文書データに対して改竄が加えられていないことが証明される。

【００９９】

ここで暗号・復号処理部１０８は、少なくともフロー制御装置２０の公開鍵を保管している。また暗号・復号処理部１０８に、各サーバやユーザの公開鍵をネットワーク上の所定の認証局等から必要に応じて取得する機能を設けることも好適である。また暗号・復号処理部１０８は、該指示入力装置１０自身の秘密鍵を

備え、該指示入力装置１０の電子署名を行うことができる。

【０１００】

上述の第３及び第４の指示送信形態（図５及び図６）の場合、各サーバ２５に送信する指示書に対する上述の暗号化処理は、この暗号・復号処理部１０８にて実行される。また、第１及び第２の指示送信形態（図３及び図４）の場合でも、フロー制御装置２０に対して送るフロー指示書５０に対する暗号化処理は、この暗号・復号処理部１０８により実行される。

【０１０１】

トークンＩ／Ｆ（インタフェース）１１０は、ユーザが保持するハードウエアトークンを受け入れ、このトークンと通信することで該ユーザの秘密鍵による電子署名を取得する機構である。ここでハードウエアトークンは、ユーザが携帯する小型の認証デバイスである。公開鍵暗号方式を利用する場合、ハードウエアトークンは、例えば、ユーザの秘密鍵データを記憶する記憶チップと、署名対象のデータに対してユーザの秘密鍵を用いて暗号化を施すことにより署名データを生成する演算回路と、署名対象のデータの入力及び署名データの出力のためのインタフェース機構とを備えるものとなる。ハードウエアトークンは、例えば接触読み取り式又は非接触読み取り式のＩＣカード、ＵＳＢ(Universal Serial Bus)等の各種有線インタフェース規格に対応したデバイス、或いはBluetooth等の各種無線インタフェース規格に対応したデバイスなどとして構成される。

【０１０２】

この構成では、通信制御部１０６は、送信すべきデータに対してユーザの電子署名を行う必要がある場合、例えばＭＤ５などの方式に従ってそのデータのメッセージダイジェストを作成し、これをトークンＩ／Ｆ１１０に装着されたハードウエアトークンに入力する。ハードウエアトークンは、入力されたメッセージダイジェストを、保持しているユーザの秘密鍵で暗号化し、その暗号化処理結果（すなわちユーザの署名）を通信制御部１０６に返す。このユーザ署名を通信制御部１０６が文書データに付加することにより、文書データに対するユーザの電子署名が為される。

【０１０３】

以上ではユーザのハードウエアトークンを利用してユーザの電子署名を行う方式を説明したが、別の方式として、指示入力装置１０内にユーザの秘密鍵を予め保管しておき、この秘密鍵を用いて上述と同様の処理により該ユーザの電子署名を行う方式も可能である。この方式では、ユーザの秘密鍵保護のため、ユーザにパスワードやバイオメトリクス等の認証情報の入力を求め、これによりユーザ認証が成功した場合に限り、そのユーザの電子署名を認めるという制御を必須とする。ハードウエアトークンを用いる構成の場合、ユーザ署名が必要な連携サービスを行うと、最悪の場合その連携サービスが完了するまで指示入力装置１０にトークンをセットしたまま待っている必要があるが、指示入力装置１０に秘密鍵を保管する構成ではそのような待機は必要ない。逆に、ハードウエアトークンを用いる構成は、ユーザは、どの複合機その他の装置からでも、ユーザ署名が必要な連携サービスを実行できるという利点がある。

【０１０４】

以上、指示入力装置１０の構成の一例を説明した。このような指示入力装置１０は、コンピュータや上述の複合機など、プログラムを実行して情報処理を実行することができる装置に、上述の各種の機能を記述したプログラムを実行させることによって実現できる。

【０１０５】

次に、フロー制御装置２０の構成について説明する。これは、上述の第１及び第２の指示送信形態（図３及び図４参照）に対応するものであり、第３及び第４の送信指示形態（図５及び図６参照）の場合は、このフロー制御装置２０は必要ない。

【０１０６】

フロー制御装置２０において、ユーザ管理部２０２は、該装置２０がサービス対象とするユーザについての各種情報を管理している。ユーザ管理部２０２が管理する情報には、例えばユーザの認証に用いる認証情報（パスワードやバイオメトリクス情報など）や、ユーザが登録しているＵＩ画面情報などがある。すなわち、本実施形態のシステムでは、ネットワーク３５上の各種サーバ装置が提供するサービスをユーザが組み合わせることで、ユーザ固有の連携サービスを定義可

能としており、これらユーザ固有の連携サービスを指示できる該ユーザ固有のＵＩ画面をフロー制御装置２０から提供する。

【０１０７】

この場合、ユーザ（個人の場合もあれば、複数人からなるグループの場合もある）が指示入力装置１０に認証情報を入力して認証が成功すると、指示入力装置１０がフロー制御装置２０に当該ユーザのＵＩ画面を要求する。この要求に応じ、フロー制御装置２０は、そのユーザが登録した連携サービスのメニュー等を含んだＵＩ画面を、そのユーザの公開鍵で暗号化した上で指示入力装置１０に送信する。ユーザが、指示入力装置１０のディスプレイに表示されたそのＵＩ画面上で、使用したい連携サービスを選択すると、その選択内容がフロー制御装置２０の公開鍵で暗号化された上で、指示入力装置１０からフロー制御装置２０に送られる。この選択結果を受けとったフロー制御装置２０は、ユーザが選択した連携サービスを示す包括指示書のひな形データを、ユーザの公開鍵で暗号化した上で、指示入力装置１０に送信する。指示入力装置１０は、この包括指示書のひな形の中に、ユーザが入力しなければならないパラメータが含まれる場合、そのパラメータの入力画面をＵＩ１０２に表示し、ユーザの入力を求める。このようにしてパラメータ群が入力されると、包括指示書が完成する。これが上述のフロー指示書５０に対応する。指示入力装置１０は、完成したフロー指示書をフロー制御装置２０の公開鍵で暗号化した上で、フロー制御装置２０に送信する。

【０１０８】

ユーザによるフロー制御装置２０への連携サービスの登録処理や、フロー制御装置２０から指示入力装置１０に提供する各ユーザ固有のＵＩ画面の情報については、本実施形態の要旨とは直接関係しないので説明を省略するが、これらについては本出願人による特願２００２－２７５２２９号、特願２００２－２７５２３０号、特願２００２－２７５２３１号に開示されているので、必要があれば参照されたい。

【０１０９】

なお、この例は、ＵＩ画面の情報や連携サービスの包括指示書のひな形はフロー制御装置２０が保管し、随時指示入力装置１０に提供する構成であったが、そ

れらＵＩ画面や包括指示書のひな形を指示入力装置１０に保管しておくこともできる。

【０１１０】

フロー制御部２０４は、ユーザが要求した連携サービスを実現するために、連携サービスにおいて規定されるフローに従って各サーバ２５や指示入力装置１０に対して必要な処理の実行依頼を行う機能モジュールである。すなわち、連携サービスは、各サーバ２５が提供する１以上の処理（以下では単位ジョブとも呼ぶ）からなるフローとして定義され、フロー制御装置２０は、このフロー定義に示される単位ジョブを順に対応するサーバに依頼していく。ここで、各サーバの処理結果は、必要に応じてフロー制御装置２０に返され、次の単位ジョブの処理対象データとしてフロー制御装置２０から対応するサーバへと送信される。フロー制御部２０４は、このような各サーバ、複合機への処理依頼と、これに対する処理結果の取得などの処理を実行する。

【０１１１】

なお、指示入力装置１０が、連携サービスの指示受付機能の他にも処理機能を備え、この処理機能を連携サービスのために提供できる場合もある。この場合、指示入力装置１０は、その処理機能についてはアプリケーションサーバ２５の１つととらえることができる。

【０１１２】

暗号・復号処理部２０６は、フロー制御装置２０からネットワーク３５に送信する文書データに対して暗号化を行ったり、送信されてきた暗号化データを復号したりする機能モジュールであり、暗号・復号処理部１０８と同等の暗号化、復号化、電子署名及びその検証の機能を有する。

【０１１３】

ここで暗号・復号処理部２０６は、指示入力装置１０や各サーバ２５などの装置や、各ユーザの公開鍵を保管しているか、又はネットワーク上の認証局等から取得する機能を備える。そして、データを送信する必要が生じた場合は、その送信先の装置やユーザの公開鍵を用いて暗号化を行う。

【０１１４】

上述の第１及び第２の指示送信形態（図３及び図４）の場合、各サーバ２５に送信する指示書に対する上述の暗号化処理は、この暗号・復号処理部２０６にて実行される。

【０１１５】

また、電子署名機能については、暗号・復号処理部２０６は、フロー制御装置２０の秘密鍵を備え、送信するデータに対してフロー制御装置２０の電子署名を付することができる。

【０１１６】

通信制御部２１２は、フロー制御装置２０とネットワーク３５上の他の装置との通信のための各種制御処理を行う機能モジュールである。

【０１１７】

以上、フロー制御装置２０の構成の一例を説明した。このようなフロー制御装置２０は、上述の各種の機能を記述したプログラムをコンピュータに実行させることによって実現できる。

【０１１８】

次にアプリケーションサーバ２５について説明する。アプリケーションサーバ２５は、該サーバが提供するサービスのためのアプリケーションプログラム２５２と、ネットワーク３５上の他の装置との通信のための制御処理を実行する通信制御部２５４と、その通信の際の暗号化及び復号の処理を実行する暗号・復号処理部２５６とを備える。

【０１１９】

サーバ２５の暗号・復号処理部２５６は、指示入力装置１０，フロー制御装置２０又は他のサーバ２５から送られてきた指示書を上述のごとく復号する機能を備える。アプリケーション２５２はその復号の結果を受け取り、これを解釈し、その解釈の結果に応じた処理を実行する。

【０１２０】

また暗号・復号処理部２５６は、該サーバ２５の処理によって得られたデータを暗号化する機能を備える。そのような処理結果のデータを、フロー制御装置２０又は他のサーバ２５に送る際には、その送り先の公開鍵を用いてそのデータを

暗号化する。

【０１２１】

また、通信制御部２５４は、上述の第１及び第２の指示送信形態（図３及び図４）では、アプリケーション２５２の処理結果をフロー制御装置２０に送信する処理を行う。また通信制御部２５４は、第３の指示送信形態（図５）では、次のサーバ２５に対する包括指示書６０（及び、必要に応じ、処理結果のデータ）を送信するための上述の処理を実行し、第４の指示送信形態（図６）では、次のサーバ２５に対する処理開始指示を送信するための上述の処理を実行する。

【０１２２】

以上説明した指示入力装置１０及びサーバ２５、及びフロー制御装置介在型のシステム構成の場合は更にフロー制御装置２０により、上述の連携サービスのフローが実現されると共に、そのフローにおける各サーバ２５への指示書の秘密を守る処理が行われる。

【図面の簡単な説明】

【図１】　連携サービスを提供するシステムの構成の一例を示す図である。

【図２】　連携サービスを提供するシステムの構成の別の例を示す図である。

【図３】　連携サービスにおける各サーバへの指示書の送信形態の一例を示す図である。

【図４】　連携サービスにおける各サーバへの指示書の送信形態の別の例を示す図である。

【図５】　連携サービスにおける各サーバへの指示書の送信形態の更に別の例を示す図である。

【図６】　連携サービスにおける各サーバへの指示書の送信形態の更に別の例を示す図である。

【図７】　紙原稿を読み取って得た文書ファイルから先頭ページのみを取り出し、これを電子メールに添付して所定の宛先に送信するという連携サービスを実現するシステムの構成例を示す図である。

【図８】　図７のシステムにおいて、指示入力装置がまず用意する平文の包

括指示書の例を示す図である。

【図９】　図９の平文の包括指示書内の個々の指示を、その指示を実行するサーバの公開鍵で暗号化した結果を示す図である。

【図１０】　入れ子構造で暗号化した包括指示書の構造を示す模式図である。

【図１１】　入れ子構造で暗号化した包括指示書の一例を示す図である。

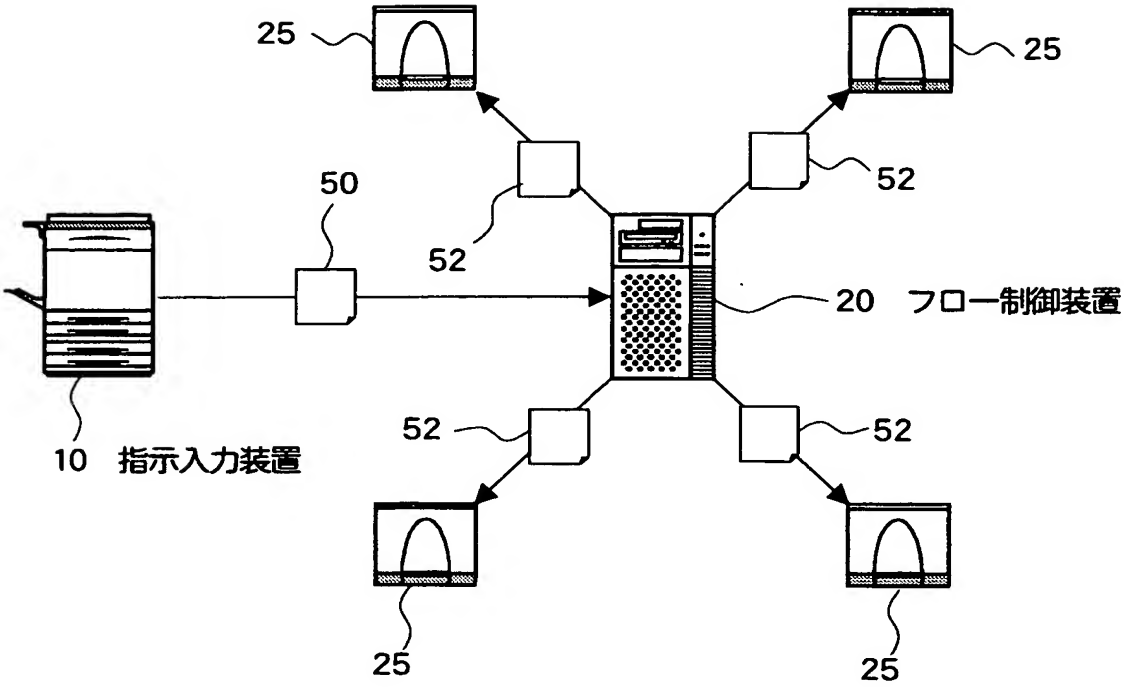
【図１２】　連携サービスを提供するシステムを構成する各装置の内部構造の例を示す図である。

【符号の説明】

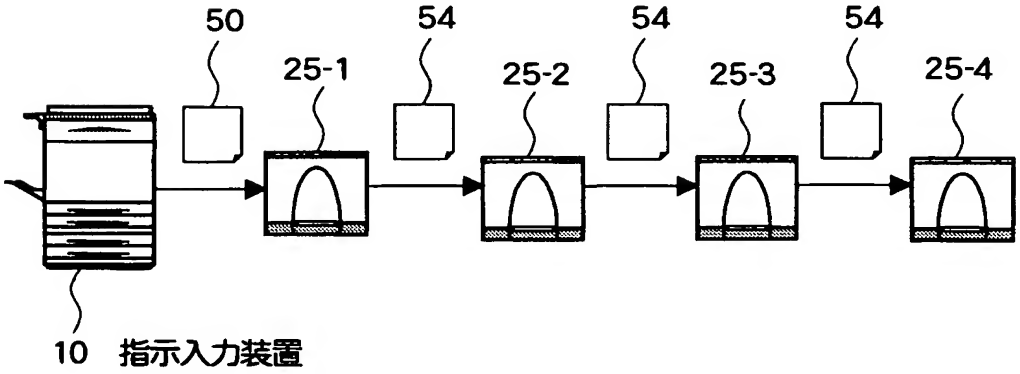
１０　指示入力装置、２０　フロー制御装置、２５　アプリケーションサーバ、５２，５４　指示書、６０　包括指示書、６２　個別指示書。

【書類名】　　図面

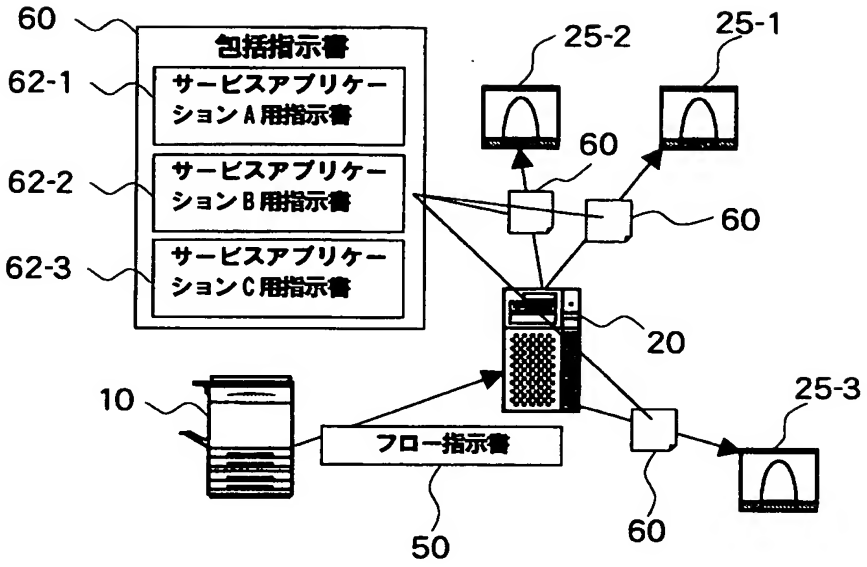
【図１】


25
25
50
52
52
20　フロー制御装置
52
52
10　指示入力装置
25
25

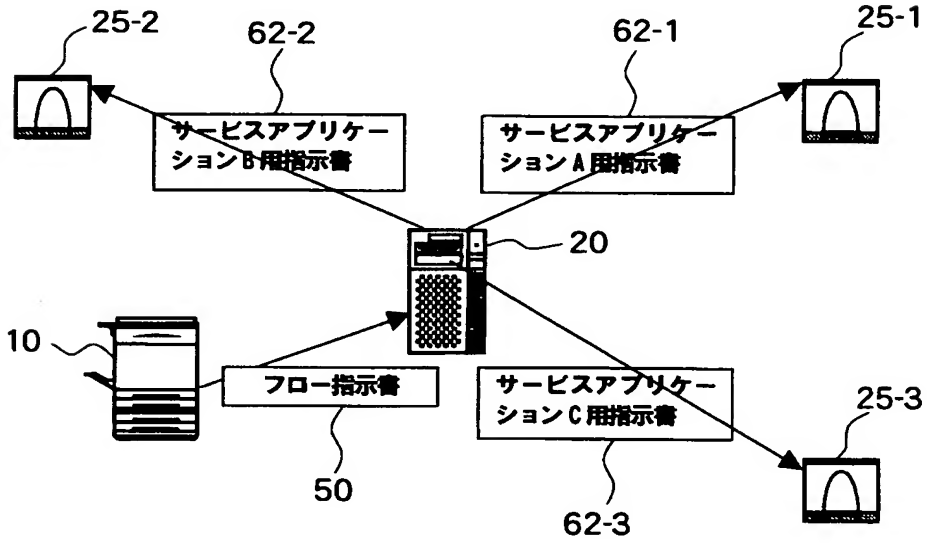
【図２】


50
54
54
54
25-1
25-2
25-3
25-4
10　指示入力装置

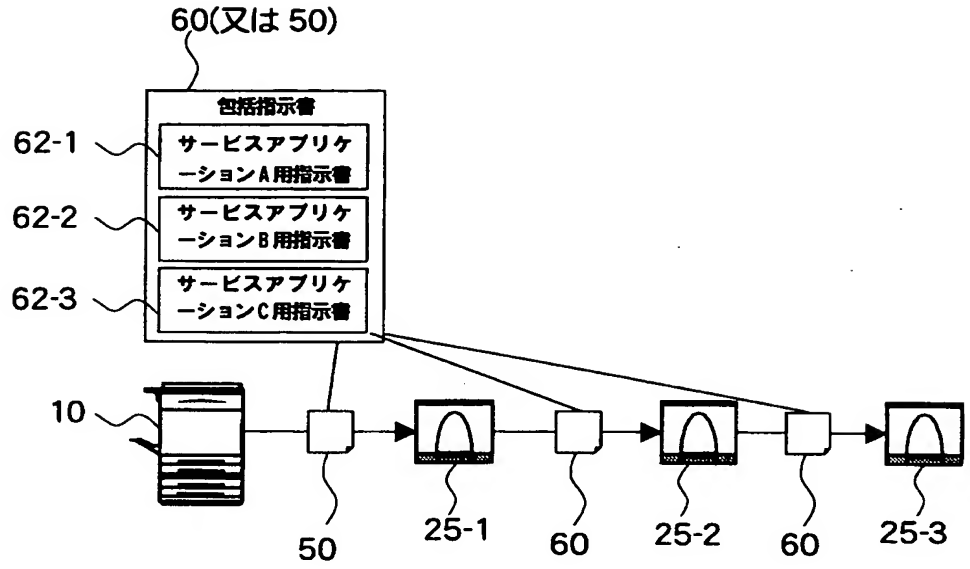
【図３】


60
包括指示書
62-1
サービスアプリケーションA用指示書
62-2
サービスアプリケーションB用指示書
62-3
サービスアプリケーションC用指示書
25-2
25-1
60
60
20
10
25-3
フロー指示書
50
60

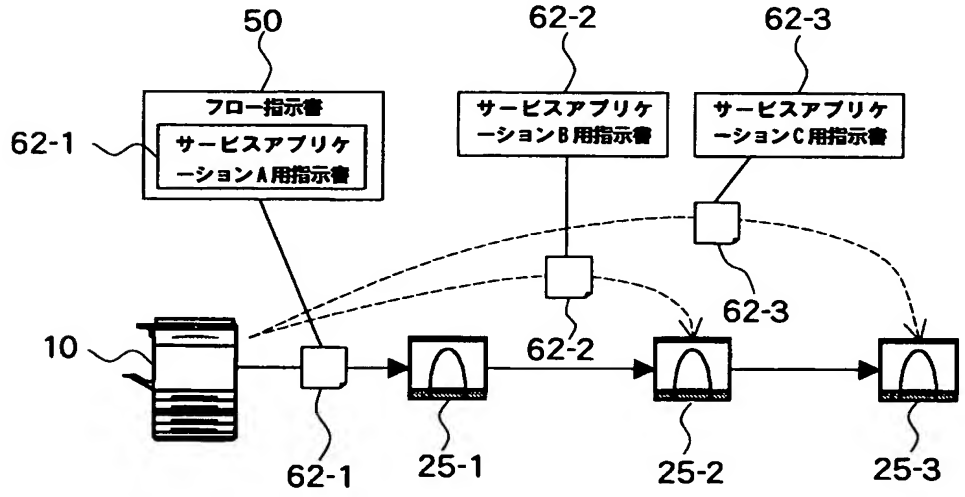
【図４】


25-2
62-2
62-1
25-1
サービスアプリケーションB用指示書
サービスアプリケーションA用指示書
20
10
フロー指示書
サービスアプリケーションC用指示書
25-3
50
62-3

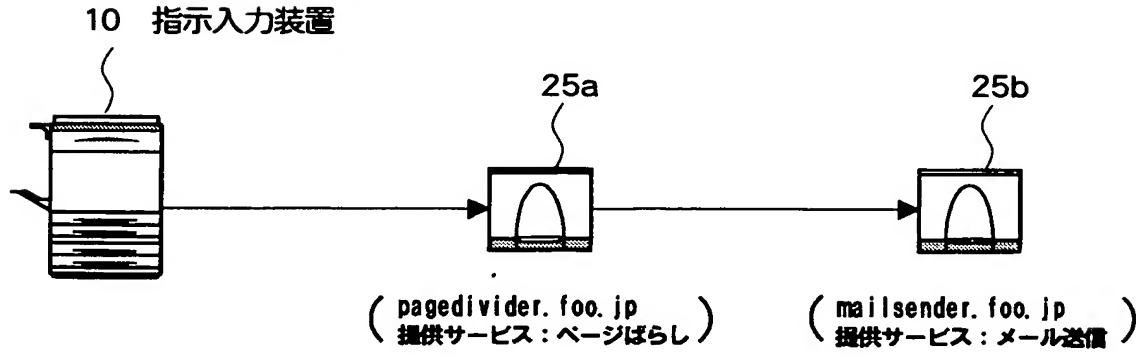
【図５】


60(又は 50)
包括指示書
62-1
サービスアプリケーションA用指示書
62-2
サービスアプリケーションB用指示書
62-3
サービスアプリケーションC用指示書
10
50
25-1
60
25-2
60
25-3

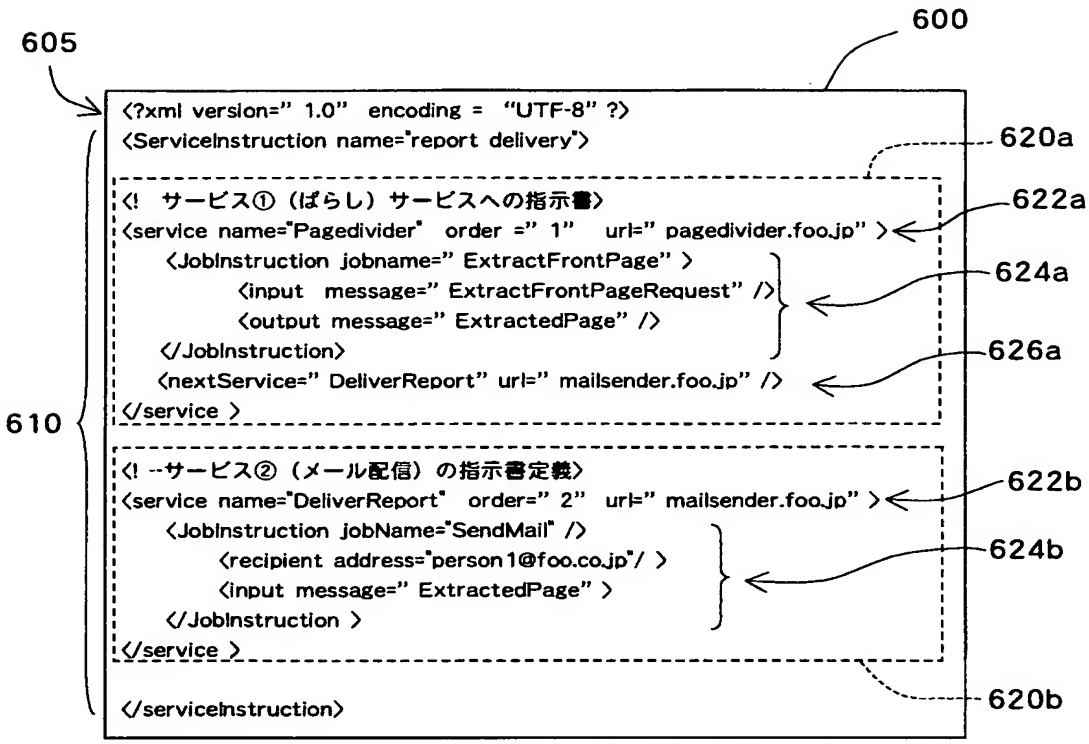
【図６】


50
62-2
62-3
フロー指示書
62-1
サービスアプリケーションA用指示書
サービスアプリケーションB用指示書
サービスアプリケーションC用指示書
10
62-3
62-2
62-1
25-1
25-2
25-3

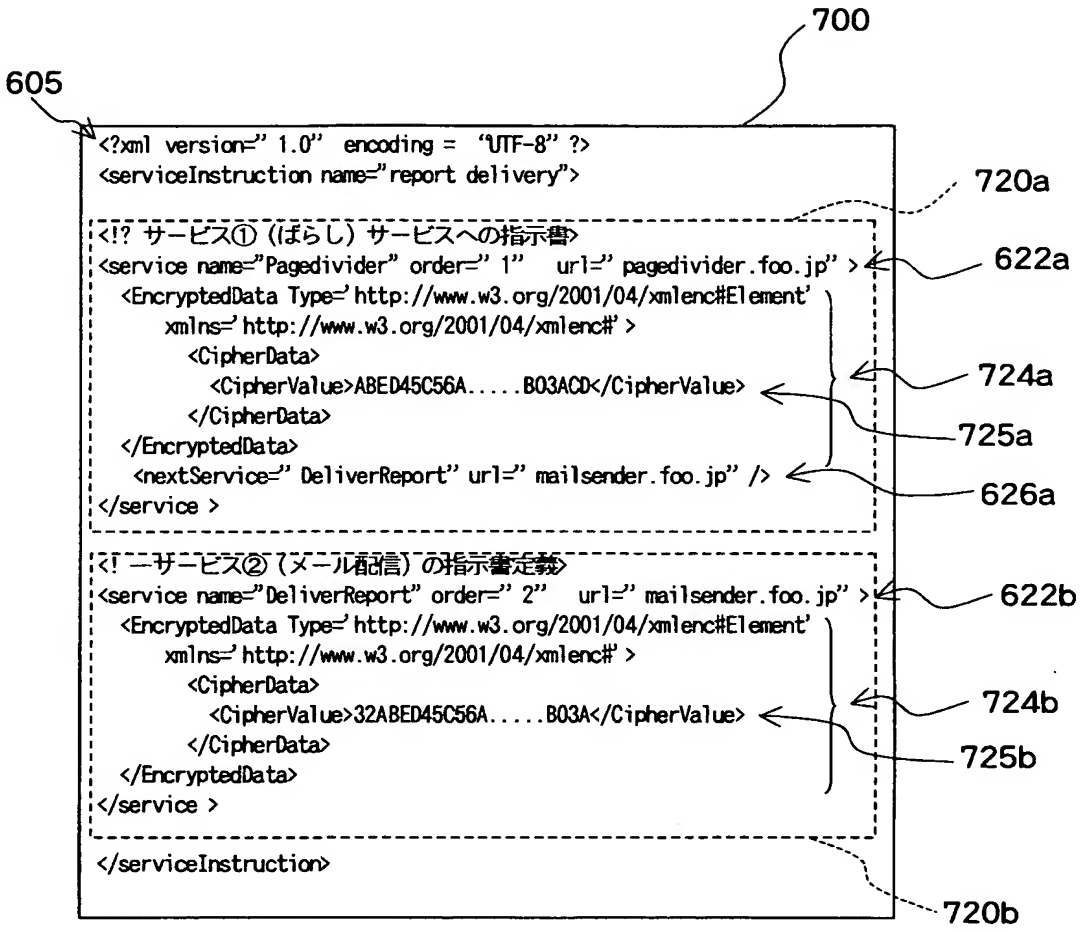
【図７】


10　指示入力装置
25a
25b
(pagedivider. foo. jp
提供サービス：ページばらし)
(mailsender. foo. jp
提供サービス：メール送信)

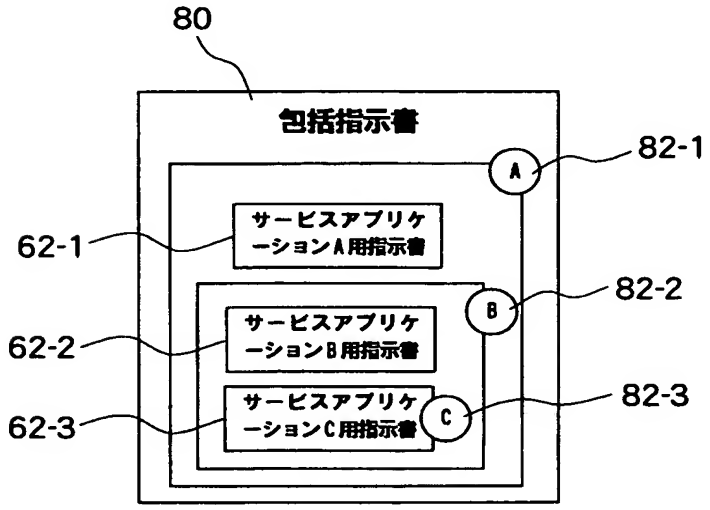
【図８】


600
605
<?xml version=" 1.0" encoding = "UTF-8" ?>
<ServiceInstruction name="report delivery">
620a
<! サービス① (ばらし) サービスへの指示書>
622a
<service name="Pagedivider" order =" 1" url=" pagedivider.foo.jp" >
<JobInstruction jobname=" ExtractFrontPage" >
624a
<input message=" ExtractFrontPageRequest" />
<output message=" ExtractedPage" />
</JobInstruction>
626a
<nextService=" DeliverReport" url=" mailsender.foo.jp" />
</service >
610
<! --サービス② (メール配信) の指示書定義>
622b
<service name="DeliverReport" order=" 2" url=" mailsender.foo.jp" >
<JobInstruction jobName="SendMail" />
624b
<recipient address="person1@foo.co.jp"/ >
<input message=" ExtractedPage" >
</JobInstruction >
</service >
620b
</ServiceInstruction>

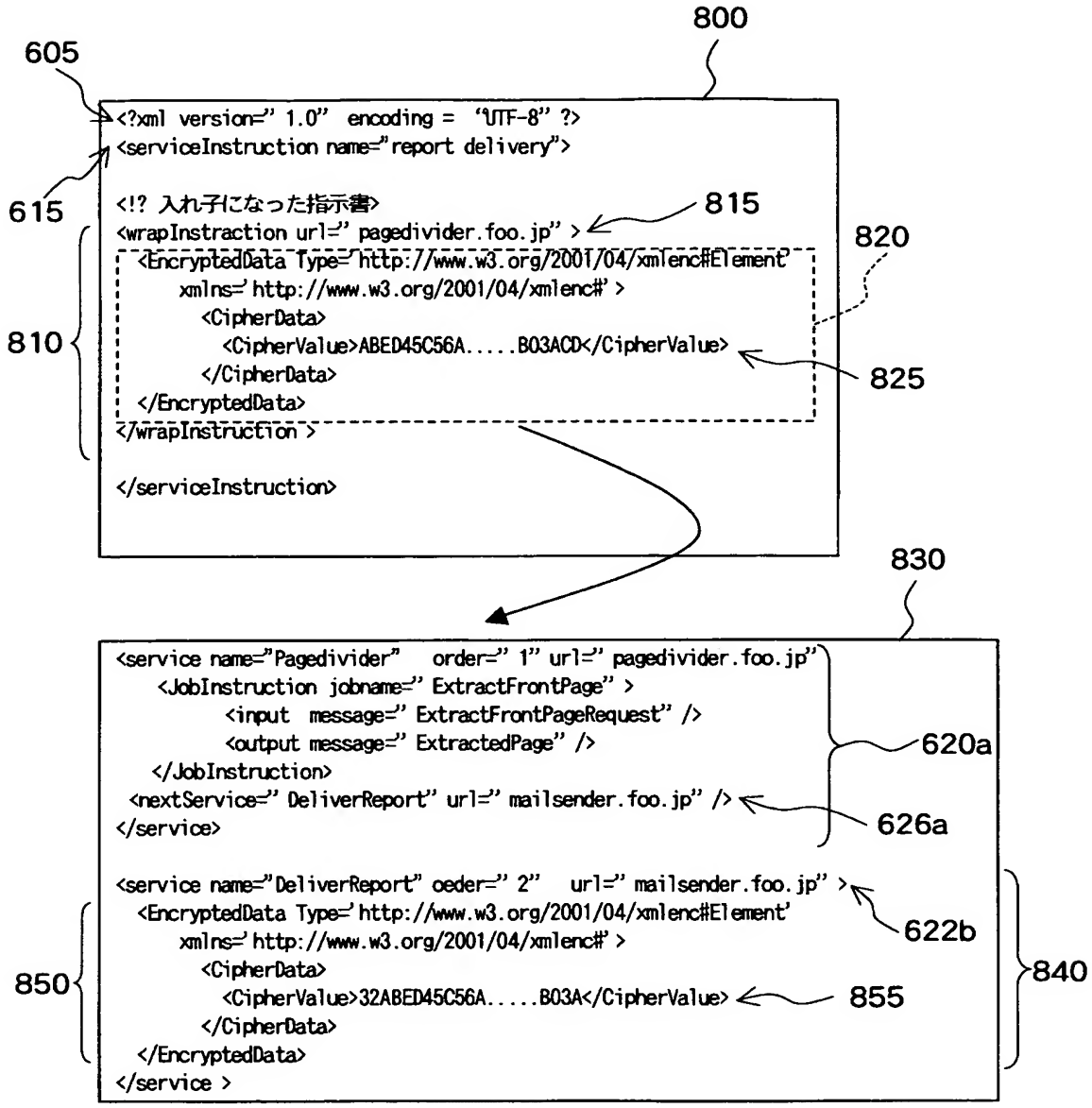
【図９】


700
605
<?xml version=" 1.0" encoding = "UTF-8" ?>
<serviceInstruction name="report delivery">
720a
<!? サービス① (ばらし) サービスへの指示書>
<service name="Pagedivider" order=" 1" url=" pagedivider.foo.jp" >
622a
<EncryptedData Type=' http://www.w3.org/2001/04/xmlenc#Element'
xmlns=' http://www.w3.org/2001/04/xmlenc#' >
<CipherData>
<CipherValue>ABED45C56A.....B03ACD</CipherValue>
724a
</CipherData>
725a
</EncryptedData>
<nextService=" DeliverReport" url=" mailsender.foo.jp" />
626a
</service >
<! ーサービス② (メール配信) の指示書定義>
<service name="DeliverReport" order=" 2" url=" mailsender.foo.jp" >
622b
<EncryptedData Type=' http://www.w3.org/2001/04/xmlenc#Element'
xmlns=' http://www.w3.org/2001/04/xmlenc#' >
<CipherData>
<CipherValue>32ABED45C56A.....B03A</CipherValue>
724b
</CipherData>
725b
</EncryptedData>
</service >
</serviceInstruction>
720b

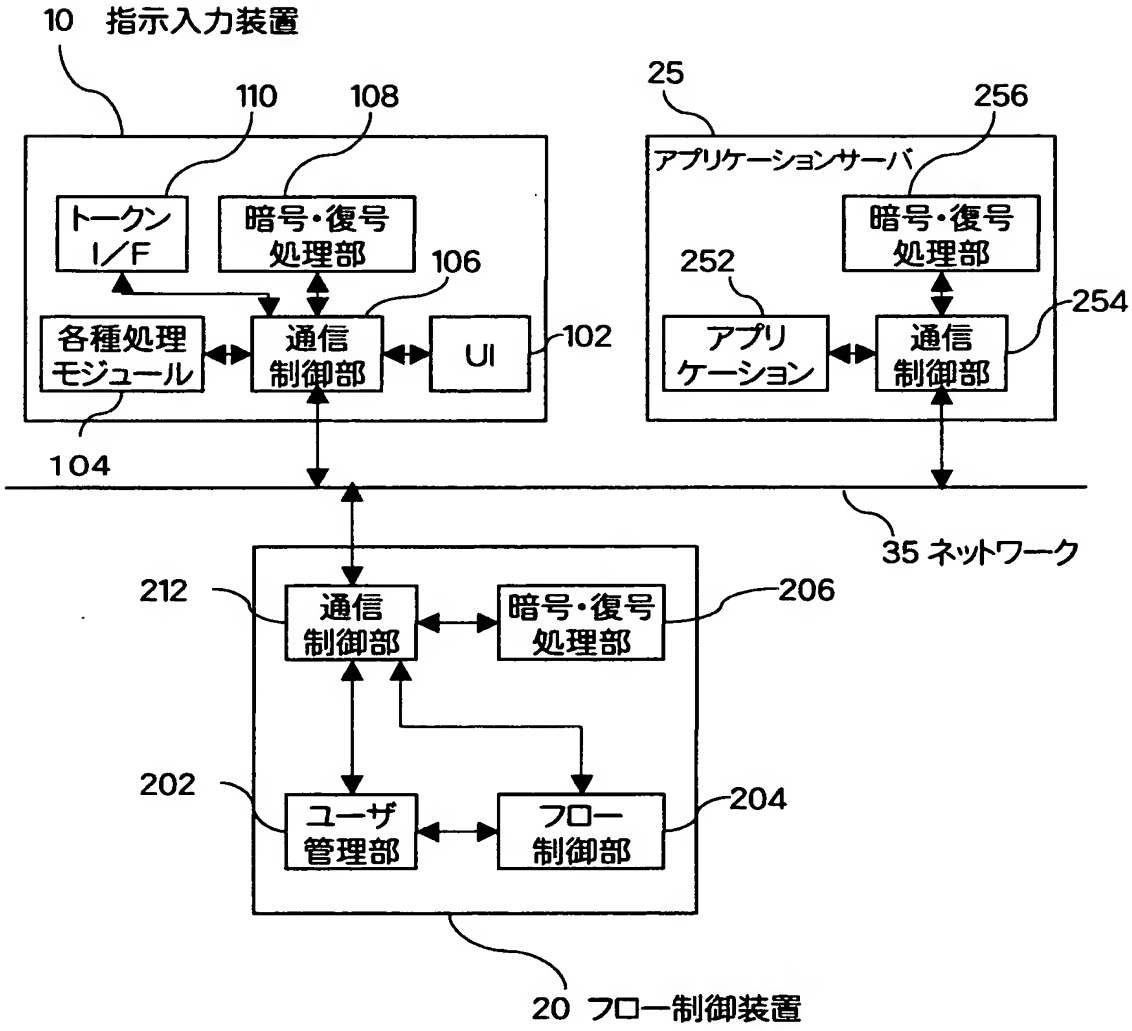
【図１０】


80
包括指示書
A
82-1
サービスアプリケーションA用指示書
62-1
B
82-2
サービスアプリケーションB用指示書
62-2
C
82-3
サービスアプリケーションC用指示書
62-3

【図１１】


800
605
615
<?xml version=" 1.0" encoding = "UTF-8" ?>
<serviceInstruction name="report delivery">
<!? 入れ子になった指示書>
<wrapInstraction url=" pagedivider.foo.jp" >
815
820
<EncryptedData Type=' http://www.w3.org/2001/04/xmlenc#Element'
xmlns=' http://www.w3.org/2001/04/xmlenc#' >
<CipherData>
<CipherValue>ABED45C56A.....B03ACD</CipherValue>
825
</CipherData>
</EncryptedData>
</wrapInstruction >
810
</serviceInstruction>
830
<service name="Pagedivider" order=" 1" url=" pagedivider.foo.jp"
<JobInstruction jobname=" ExtractFrontPage" >
<input message=" ExtractFrontPageRequest" />
<output message=" ExtractedPage" />
620a
</JobInstruction>
<nextService=" DeliverReport" url=" mailsender.foo.jp" />
626a
</service>
<service name="DeliverReport" oeder=" 2" url=" mailsender.foo.jp" >
622b
<EncryptedData Type=' http://www.w3.org/2001/04/xmlenc#Element'
xmlns=' http://www.w3.org/2001/04/xmlenc#' >
<CipherData>
<CipherValue>32ABED45C56A.....B03A</CipherValue>
855
</CipherData>
</EncryptedData>
</service >
850
840

【図１２】


10　指示入力装置
110
108
トークン I/F
暗号・復号処理部
106
各種処理モジュール
通信制御部
UI
102
104
25
256
アプリケーションサーバ
暗号・復号処理部
252
254
アプリケーション
通信制御部
35 ネットワーク
212
通信制御部
暗号・復号処理部
206
202
ユーザ管理部
フロー制御部
204
20 フロー制御装置

【書類名】　　要約書

【要約】

【課題】　各サーバへの指示を示した指示書をそれらサーバ間で受け渡しながら、各サーバが指示書内の各自の指示を実行することで、１つのサービスを提供するシステムにおいて、指示書に示された各サーバへの指示の秘密を守る。

【解決手段】　サーバ２５ａが提供するページばらし（複数ページを含む文書のファイルから所定のページを抜き出し、そのページのファイルを出力する処理）と、サーバ２５ｂが提供する電子メール送信処理とを組み合わせることで、ユーザが指示入力装置１０に投入した文書のファイルから、先頭ページを抜き出して、所定の宛先に電子メールで送信するという連携サービスを提供することを考える。指示入力装置１０は、各サーバ２５ａ、２５ｂの処理内容の記述を、それぞれ対応するサーバ２５ａ、２５ｂの公開鍵で暗号化し、その各々の暗号化結果を含んだ指示書を作成して、サーバ２５ａに送信する。

【選択図】　　図７

特願２００３－０８１９１８

出　願　人　履　歴　情　報

識別番号　　［０００００５４９６］

１．変更年月日　　１９９６年　５月２９日
［変更理由］　　住所変更
住　所　　東京都港区赤坂二丁目１７番２２号
氏　名　　富士ゼロックス株式会社